CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

15 Juni 2022

EDISI 105

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	1	0	0
URGENT	0	2	2
IMPORTANT	1	0	0

General News

Polisi Memperingatkan *Phishing Scam* Baru yang Melibatkan Iklan Layanan Kebersihan di Media Sosial

Jenis penipuan baru berupa *phishing scam* telah muncul dengan memasang *malware* di ponsel korban untuk mencuri kredensial perbankan korban. Dalam penipuan itu, orang akan menerima iklan layanan kebersihan melalui pesan. Korban akan diminta melakukan pembayaran dengan mengunduh aplikasi melalui tautan yang dikirimkan kepada mereka. Tautan ini hanya dikirim setelah korban memutuskan untuk menggunakan layanan. Tetapi aplikasi tersebut diyakini mengandung *malware*. Setelah melakukan instalasi aplikasi, korban akan diminta untuk melakukan pembayaran melalui situs perbankan yang sah menggunakan informasi perbankan *online* mereka. Setidaknya dua orang telah menjadi korban penipuan dengan total kerugian mencapai $2.000 bulan ini. Oleh karena itu, Polisi menganjurkan masyarakat untuk mengunduh file langsung dari sumber resmi dan terverifikasi guna memastikan file terbebas dari malware ataupun virus.

Prioritas: *3. Important*

< https://www.straitstimes.com/singapore/police-warn-of-new-phishing-scam-involving-cleaning-services-ads-on-social-media-platforms >

Android *Malware* di Google Play Store Telah Diunduh Sebanyak 2 Juta Unduhan

Peneliti keamanan siber telah menemukan adanya *adware* dan *malware* pencuri informasi di Google Play Store bulan lalu namun setidaknya sejumlah lima *adware* dan *malware* masih tersedia dan telah mengumpulkan lebih dari dua juta unduhan. Infeksi *adware* menyebabkan iklan yang tidak diinginkan muncul sehingga sangat mengganggu. Selain itu, *adware* ataupun *malware* yang terunduh menurunkan pengalaman pengguna, menguras baterai, dan menghasilkan panas. Perangkat lunak ini mencoba bersembunyi dengan menyamar sebagai sesuatu yang lain pada perangkat *host* dan menghasilkan uang untuk operator jarak jauh. Di antara sekian banyak ancaman yang berhasil menyusup ke Google Play Store, berikut merupakan 5 ancaman yang masih ada: PIP Pic Camera Photo Editor, Wild & Exotic Animal Wallpaper, ZodiHoroscope, PIP Camera 2022, dan Magnifier Flashlight.

Prioritas: *1. Critical*

< https://www.bleepingcomputer.com/news/security/android-malware-on-the-google-play-store-gets-2-million-downloads/ >

Data Breach

70.000 Catatan Perawatan Kesehatan Pasien Kaiser Permanente Mengalami Data Breach

Informasi pribadi hingga catatan perawatan kesehatan dari 70.000 pasien Kaiser Permanente di negara bagian Washington telah bocor setelah adanya akses tidak sah ke sistem *e-mail* milik perawatan kesehatan AS. Insiden pembobolan data tersebut terjadi pada awal April dan berpotensi mengungkap nama pasien, nomor rekam medis, tanggal layanan, dan informasi hasil tes laboratorium. Meskipun tidak ada bukti pencurian identitas atau penyalahgunaan informasi kesehatan, Kaiser Permanente tetap menyarankan pihak yang terkena dampak untuk waspada terhadap potensi penipuan.

Prioritas: *2. Urgent*

< https://portswigger.net/daily-swig/kaiser-permanente-data-breach-exposed-healthcare-records-of-70-000-patients?&web_view=true >

Rumah Sakit Arizona Mengatakan Bahwa Sebanyak 700.000 *Social Security Number* Mengalami Kebocoran Akibat *Ransomware Attack*

Serangan ransomware terhadap organisasi layanan kesehatan terus berlanjut sepanjang tahun 2021 dan 2022. Sebuah rumah sakit besar di Yuma, Arizona

mengirimkan surat pemberitahuan terkait dengan adanya *data breach* kepada lebih dari 700.000 pasien setelah serangan *ransomware* pada bulan April yang berdampak pada bocornya nomor jaminan sosial pasien. Dalam surat kepada para korban yang baru-baru ini dipublikasikan, Yuma Regional Medical Center (YRMC) mengatakan telah menemukan serangan *ransomware* pada 25 April dan segera membuat sistem *offline* sebelum menghubungi pakar keamanan siber dan penegak hukum.

Prioritas: *2. Urgent*

< https://therecord.media/arizona-hospital-says-ssns-of-700000-people-leaked-during-april-ransomware-attack/?web_view=true >

Vulnerabilities

Side-Channel Attack Baru Bernama Hertzbleed Memengaruhi Intel, CPU AMD

Side-Channel Attack baru bernama Hertzbleed memungkinkan penyerang jarak jauh untuk mencuri kunci kriptografi dengan mengamati variasi frekuensi CPU yang diaktifkan oleh tegangan dinamis dan penskalaan frekuensi (DVFS). Ini dimungkinkan karena pada prosesor x86 Intel (CVE-2022-24436) dan AMD (CVE-2022-23823) modern, penskalaan frekuensi dinamis bergantung pada konsumsi daya dan data yang sedang diproses. DVFS adalah fitur manajemen daya yang digunakan oleh CPU modern untuk memastikan bahwa sistem tidak melampaui batas termal dan daya selama beban tinggi, serta untuk mengurangi konsumsi daya keseluruhan selama beban CPU rendah. Intel mengatakan kelemahan ini memengaruhi semua prosesornya sedangkan AMD mengungkapkan bahwa Hertzbleed memengaruhi beberapa produknya. Menurut tim peneliti di belakang Hertzbleed, Intel dan AMD tidak memiliki rencana untuk merilis patch untuk mengatasi Hertzbleed.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/new-hertzbleed-side-channel-attack-affects-intel-amd-cpus/ >

Pembaruan Windows 11 KB5014697 Menambahkan *Spotlight* untuk Desktop Serta Memperbaiki 33 *Bug*

Microsoft telah merilis pembaruan Windows 11 KB5014697 dengan melakukan *security update*, *improvements*, dan fitur *Spotlight* untuk Desktop yang secara otomatis mengubah latar belakang desktop Anda. KB5014697 adalah pembaruan kumulatif wajib yang berisi pembaruan keamanan untuk kerentanan yang ditemukan di bulan-bulan sebelumnya. Pembaruan kumulatif Windows 11 KB5014697 mencakup sekitar 35 peningkatan dan perbaikan termasuk di antaranya: mengatasi masalah yang

menyebabkan penyalinan file menjadi lebih lambat serta mengatasi masalah yang memengaruhi *rendering* pada Widgets *icon default* pada taskbar.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/microsoft/windows-11-kb5014697-update-adds-spotlight-for-desktop-fixes-33-bugs/ >